I. PATENT ABSTRACTS OF JAPAN

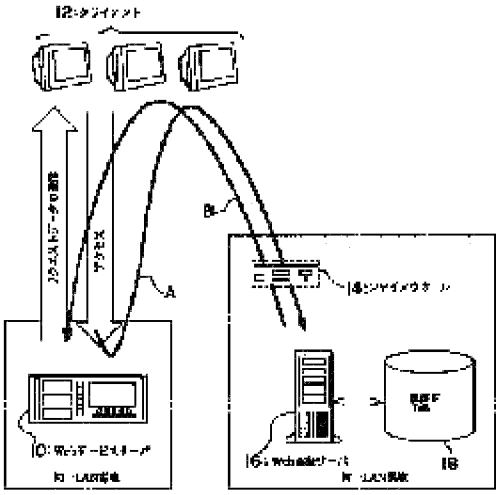
(11)Publication number : **11-282804**
(43)Date of publication of application : **15.10.1999**

(51)Int.Cl. G06F 15/00
H04L 9/32
H04L 12/54
H04L 12/58

(21)Application number : **10-085319**
(22)Date of filing : **31.03.1998**

(71)Applicant : **SECOM JOHO SYSTEM KK**
(72)Inventor : **HIRAI SHIGERU**

(54) COMMUNICATION SYSTEM HAVING USER AUTHENTICATION FUNCTION AND USER AUTHENTICATION METHOD



(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication system which can improve independence and versatility of both service and authentication servers and also can easily secure the common use of the authentication server among plural services.
SOLUTION: When an access is given from a client 12 which does not finish authentication of a user yet, a Web page including a redirect request is returned to the client 12 to access a Web server 16 and then to finish the authentication of the user. If the client 12 receives the Web page and accesses the server 16, the server 16 performs necessary authentication processing. If the server 16 succeeds in authentication processing, the server 16 sets this fact at a cookie and returns a prescribed Web page to the client 12. In this case, a redirect request can be included in a Web page to access again a Web service server 10. As a result, the direct accesses can be eliminated to both servers 10 and 16 and accordingly both reliability and versatility of the server 16 can be improved.

CLAIMS

[Claim(s)]

[Claim 1]In an included system, a service server, an authentication server, and a client which were connected on a network so that communication to mutual was possible said service server, When access is received from said client which has not finished required user authentication, Including a means to transmit redirect request information required as accessing said authentication server to this client, said authentication server, A communications system characterized by what user authentication of this client is performed when there is access from said client, and a means to transmit information that it means that user authentication was successful when said user authentication was successful and that it attests to said client is included for.

[Claim 2]A communications system characterized by what said means contained in said authentication server transmits for redirect request information required as accessing said service server collectively when transmitting said information that it attests to said client in the communications system according to claim 1.

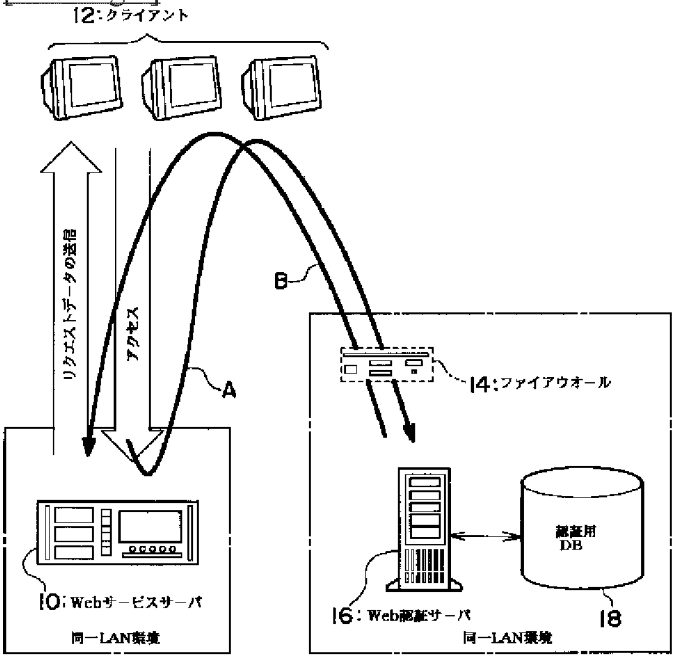
[Claim 3]A communications system, wherein said client contains a means to access said service server or said authentication server when redirect request information is received from said service server or said authentication server, in the communications system according to claim 1 or 2.

[Claim 4]In the communications system according to any one of claims 1 to 3, said client, A communications system by which a means to transmit said information that it attests to this service server in the case of access to said service server being further included when said information that it attests is already received from said authentication server.

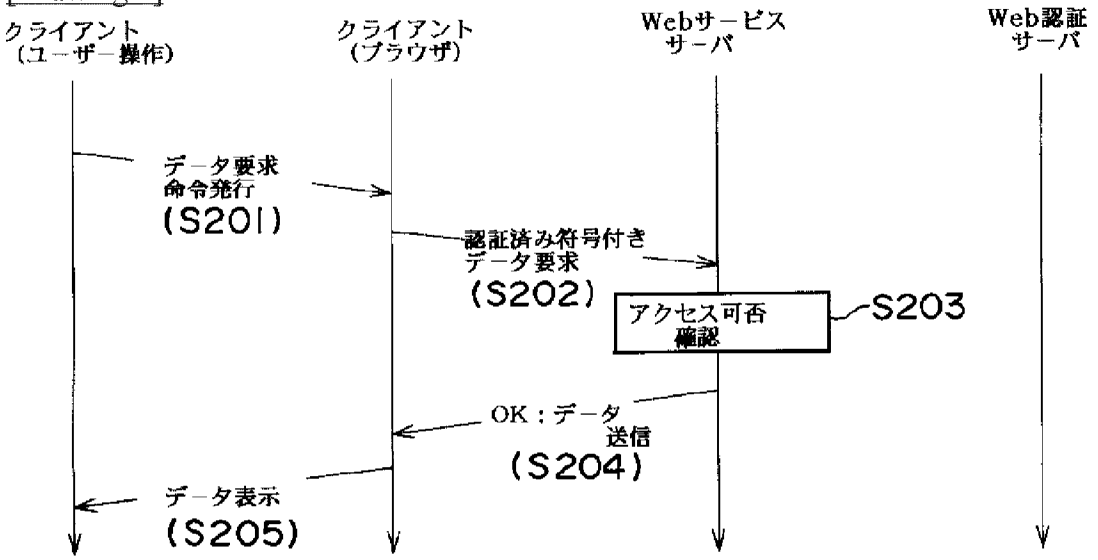
[Claim 5]A service server, an authentication server which were connected on a network so that communication to mutual was possible, And it is the method of performing user authentication of said client in a system containing a client, When access is received from said client which has not finished required user authentication with said service server, Redirect request information required as accessing said authentication server to this client is transmitted, A user authentication method characterized by what user authentication of this client is performed when there is access from said client in said authentication server, and information showing user authentication having been successful when said user authentication was successful is transmitted for to said client.

DRAWINGS

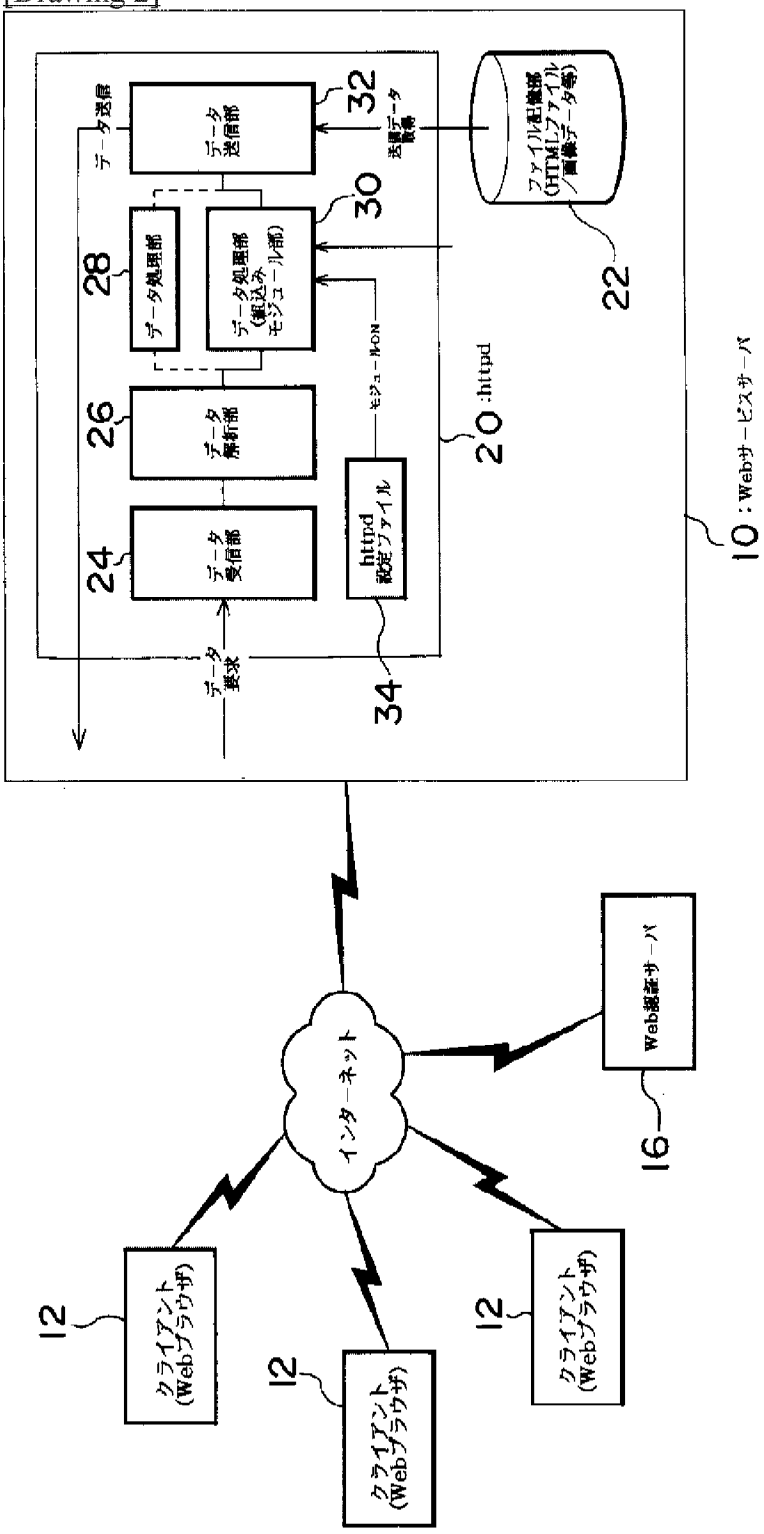
[Drawing 1]



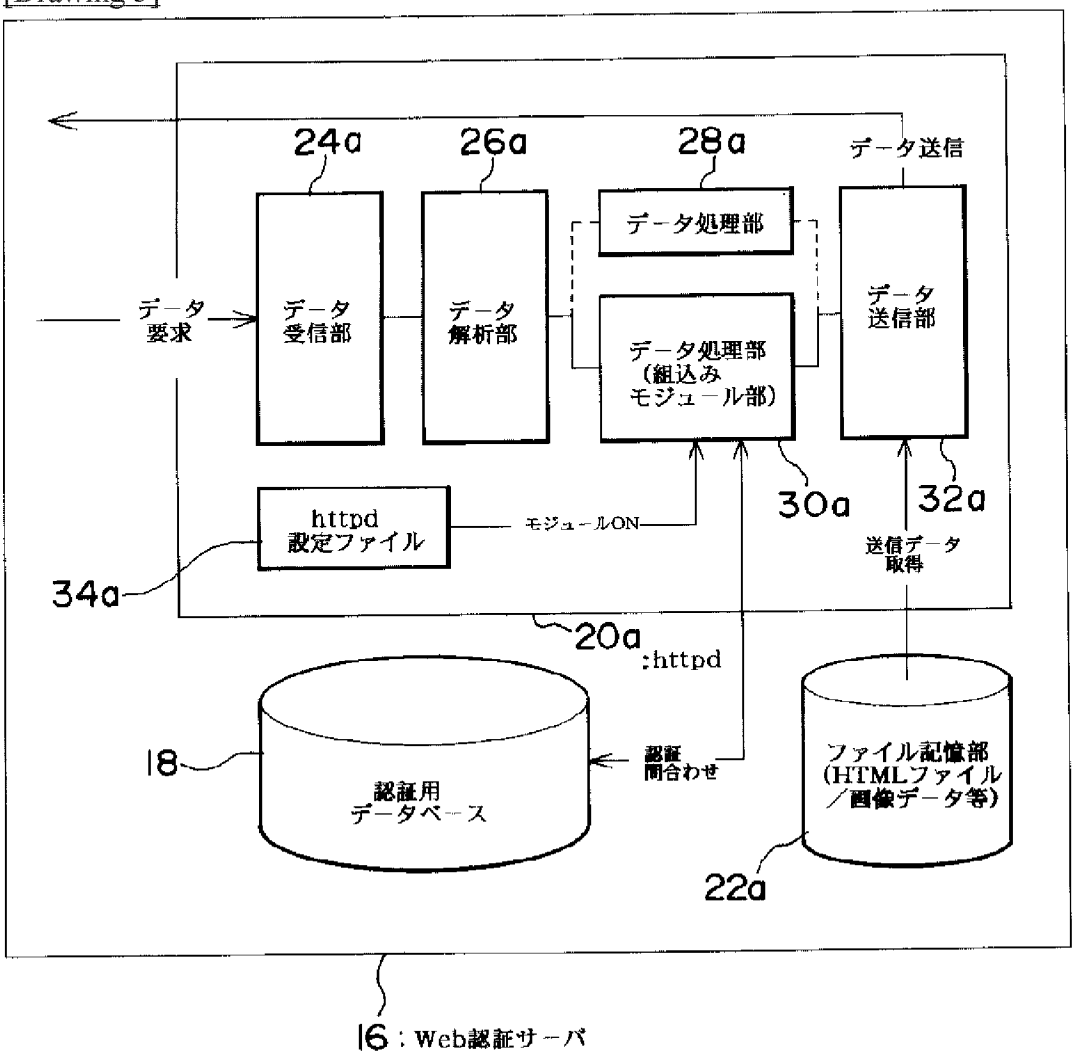
[Drawing 5]



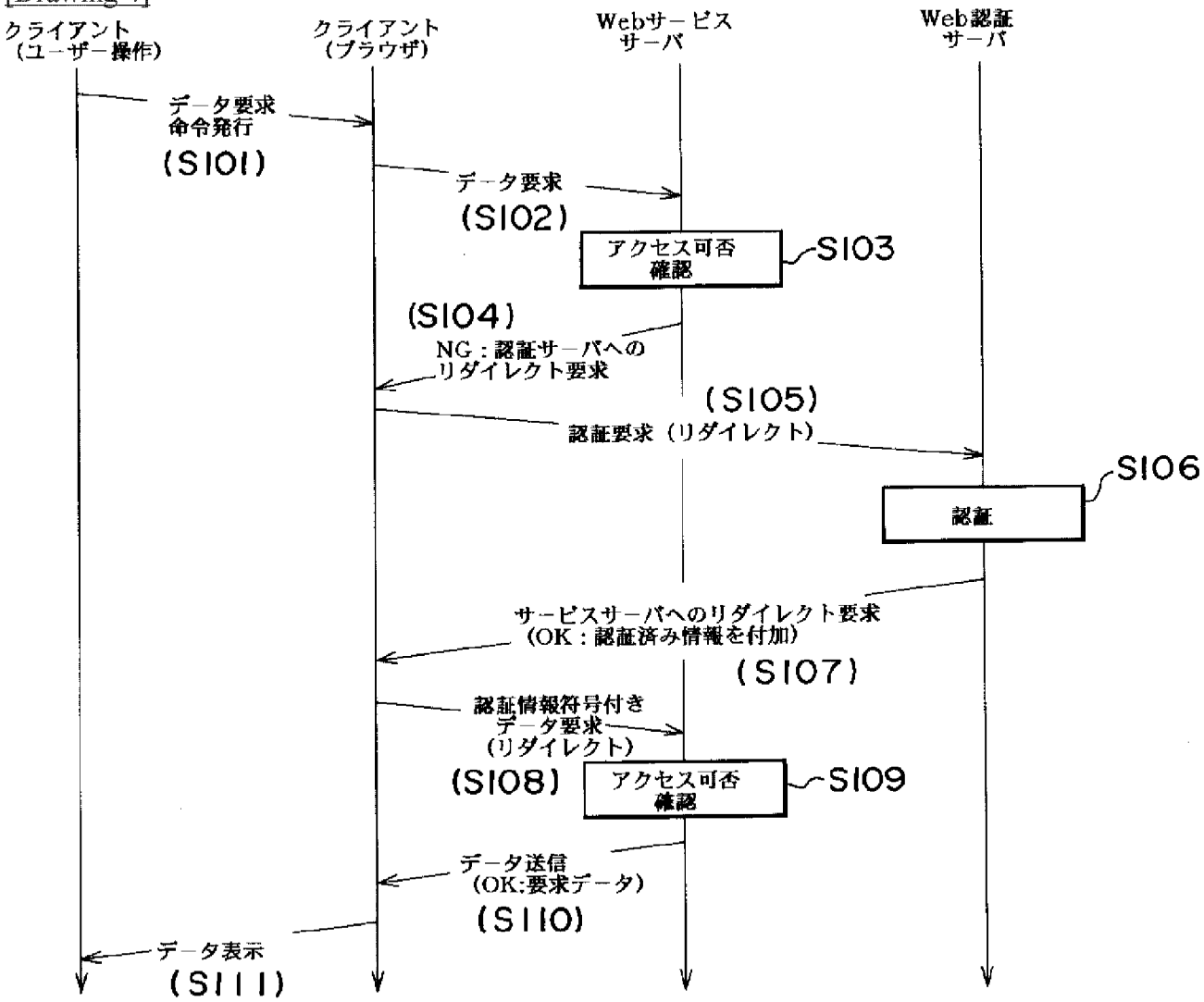
[Drawing 2]


10：Webサーバシステム
20 :httpd
22
24
26
28
30
32
34
データ送信部
データ処理部
データ処理部（組込みモジュール部）
データ解析部
データ受信部
httpd設定ファイル
ファイル記憶部（HTMLファイル／画像データ等）
データ送信
データ要求
モジュールON
インターネット
Web検索サーバ
16
クライアント（Webブラウザ）
12

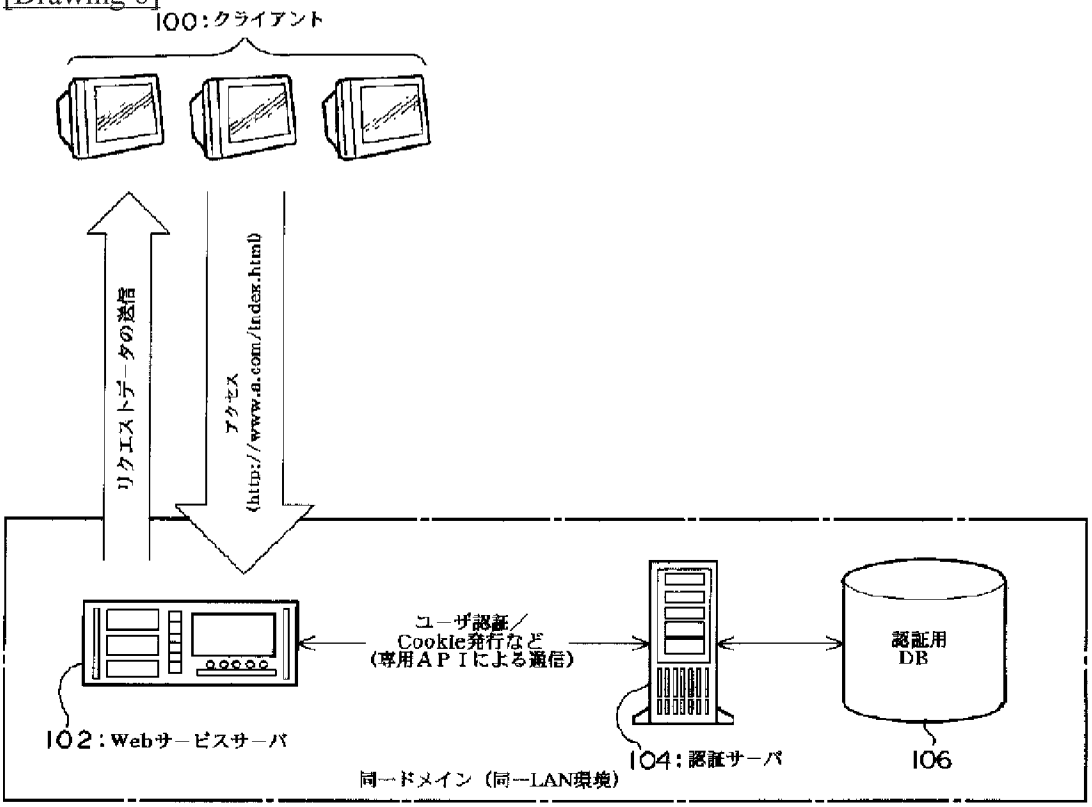
[Drawing 3]


24a
26a
28a
データ送信
データ処理部
データ
要求
データ
受信部
データ
解析部
データ処理部
(組込み
モジュール部)
データ
送信部
30a
32a
httpd
設定ファイル
モジュールON
送信データ
取得
34a
20a
:httpd
18
認証用
データベース
認証
問合わせ
ファイル記憶部
(HTMLファイル
/画像データ等)
22a
16：Web認証サーバ

[Drawing 4]


クライアント
(ユーザー操作)
クライアント
(ブラウザ)
Webサービス
サーバ
Web認証
サーバ
データ要求
命令発行
(S101)
データ要求
(S102)
アクセス可否
確認
S103
(S104)
NG：認証サーバへの
リダイレクト要求
(S105)
認証要求（リダイレクト）
S106
認証
サービスサーバへのリダイレクト要求
(OK：認証済み情報を付加)
(S107)
認証情報符号付き
データ要求
(リダイレクト)
(S108)
アクセス可否
確認
S109
データ送信
(OK:要求データ)
(S110)
データ表示
(S111)

[Drawing 6]


100：クライアント
リクエストデータの送信
アクセス
(http://www.a.com/index.html)
ユーザ認証／
Cookie発行など
（専用ＡＰＩによる通信）
認証用
DB
102：Webサービスサーバ
104：認証サーバ
106
同一ドメイン（同一LAN環境）

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]Especially this invention relates to the art which improves the flexibility of an authentication server in the user authentication between the client/servers connected to the network about a communications system with a user authentication function, and a user authentication method.
[0002]
[Description of the Prior Art]In recent years, the communication environment using World Wide Web (WWW) has spread quickly, and not only use with a mere scientific level but commercial use, such as on-line shopping and commercial database service, has spread quickly. And in order to carry out commercial use of the WWW completely in this way, it is indispensable to establish the art of performing user authentication of a reliable client at the Web server side, and, for this reason, various kinds of art is proposed.
[0003]Drawing 6 is a figure explaining the structure of attestation of the client of a service server with the authentication server in WWW generally considered conventionally. As shown in the figure, in WWW, the client 100 which carries a web browser by sending out URL (Uniform Resource Locater) to the Internet, The resource (hypertext) specified by this URL can be acquired and desired image display can be obtained on a display.
[0004]Under the present circumstances, if the resource which the client 100 specified by URL is related with the service which is stored in Web service server 102 and needs user authentication, This Web service server 102 sends the hypertext which searches for the certification information of user ID, a password, etc. to the client 100. And according to this, the client 100 transmits predetermined certification information to this Web service server 102.
[0005]In this way, Web service server 102 which received certification information from the client 100, While transmitting the received certification information to the authentication server 104 usually installed in the same domain, i.e., the same LAN environment, using an application interface (API) for exclusive use, user authentication processing is requested. The authentication server 104 which received this request performs user authentication, referring to the various certification information stored in the database 106 for attestation. And if it is checked that it succeeds in attestation and he is a regular user, Cookie (Cookie) showing the client 100 concerned being user authentication ending will be published so that the subsequent communication with Web service server 102 and the client 100 may be presented. This Cookie is information included in that header part when replying the hypertext from Web service server 102.
Henceforth, access from the client 100 holding the Cookie of predetermined contents is received, The hypertext of a user desire is replied to the client 100, without judging that Web service server 102 is access from the client 100 which has already finished user authentication, and performing user authentication in the authentication server 104 anew.

[0006]
[Problem(s) to be Solved by the Invention]according to the user authentication art of the general former in which it explained above, being able to perform user authentication based on the

certification information transmitted from the client 100, and facing the commercial use of WWW -- necessity -- it becomes possible to secure sufficient security.
[0007]However, according to the above-mentioned conventional art, the authentication server 104 is not what was built as a Web server, Web service server 102 used as a front end and the authentication server 104 used as a back end need a deep dependency, and a request of attestation and the software for exclusive use for a result notice are installed in both in many cases. For this reason, even if it built the highly efficient authentication server 104, it was difficult to use this with other Web service servers, and construction of the efficient system which carries out common use of the authentication server 104 with two or more services was difficult.
[0008]This invention is made in light of the above-mentioned problems, the purpose improves the independency and flexibility of a service server and an authentication server, and there is carrying out common use of the authentication server with two or more services in providing an easy authentication system.
[0009]
[Means for Solving the Problem](1) In order to solve an aforementioned problem, this invention, In an included system, a service server, an authentication server, and a client which were connected on a network so that communication to mutual was possible said service server, When access is received from said client which has not finished required user authentication, Including a means to transmit redirect request information required as accessing said authentication server to this client, said authentication server, When there is access from said client, user authentication of this client is performed, and when said user authentication is successful, a means to transmit information showing user authentication having been successful to said client is included.
[0010](2) In one mode of this invention, when said means contained in said authentication server transmits said information showing user authentication having been successful to said client, it transmits redirect request information required as accessing said service server collectively.
[0011](3) In a mode of further others of this invention, said client contains a means to access said authentication server or said service server, when redirect request information is received from said service server or said authentication server.
[0012](4) In other modes of this invention, said client contains further a means to transmit said information that it attests to this service server in the case of access to said service server, when said information that it attests is already received from said authentication server.
[0013]
[Embodiment of the Invention]Hereafter, an embodiment of the invention is described in detail based on a drawing.
[0014]Drawing 1 is a figure explaining the outline of the authentication system concerning an embodiment of the invention. Web service server 10 and the client 12 to which the Web system was connected on the Internet in the figure, It is constituted including the Web authentication server 16 similarly connected to the Internet via the firewall 14, and Web service server 10, the client 12, and the Web authentication server 16 are mutually connected so that communication is possible. The Web authentication server 16 can access now the database 18 for attestation installed in the same LAN environment.
[0015]When the client 12 which carries a web browser accesses Web service server 10 which has not finished still effective user authentication in the Web system shown in the figure, This Web service server 10 transmits the Web page which includes a redirect request to the client 12,

and it is required that the Web authentication server 16 should be accessed anew. In the client 12, as this redirect request is interpreted and it is shown in the figure Nakaya seal A, the Web authentication server 16 is automatically accessed without a user's interference.
[0016]When the hypertext in which a "redirect request" is included is received in many web browsers, By interpreting that demand, being able to reload a specification Web page now automatically, and utilizing this function fully in this authentication system, The direct communication with Web service server 10 and the Web authentication server 16 was abandoned, and it has succeeded in improving the flexibility of the Web authentication server 16.
[0017]Then, as it is shown in the arrow A, if the client 12 redirects the demand of Web service server 10 and accesses the Web authentication server 16, the Web authentication server 16 will be tested by comparison in the database 18 for attestation, and will perform user authentication.
[0018]If it succeeds in user authentication by the Web authentication server 16 here, this Web authentication server 16 will transmit the Web page which includes another redirect request to the client 12, and it will be required that Web service server 10 should be accessed anew shortly. Under the present circumstances, the information which shows a purport [finishing / user authentication] in this Web page is set as Cookie. And Web service server 10 transmits the Web page which a user wishes to the client 12 by what Web service server 10 receives for URL included the contents of this Cookie.
[0019]Since direct access does not occur from Web service server 10 to the Web authentication server 16 in this authentication system, the interface between these Web service servers 10 and the Web authentication server 16 can be made very brief. Thereby, the independency and flexibility of a service server and an authentication server can be improved, and common use of the authentication server can be easily carried out with two or more services.
[0020]moreover -- this authentication system -- the Web authentication server 16 and Web service server 10 -- each -- the Internet top -- IP -- it being installed, ****ing and so that it may be accessible, For example, it may prevent from accessing the Web authentication server 16 from the outside besides passing the firewall 14. It is not necessary to necessarily install the Web authentication server 16 and Web service server 10 in the same LAN environment like conventional technology. for this reason -- the same -- the Internet top -- IP -- user authentication can be easily requested to the Web authentication server 16 from other Web service servers 10 installed so that it might be accessible.
[0021]Hereafter, it explains still in detail about the composition and the authentication procedure of this authentication system.
[0022]Drawing 2 is a figure showing the composition of Web service server 10 with the entire configuration of this communications system. As shown in the figure, Web service server 10, Have httpd(Hyper Text Transfer Protocol Daemon) 20 and the file storing part 22, and to httpd20. The data receiving section 24, the data analysis part 26, the data processing parts 28 and 30, the data transmission part 32, and the httpd configuration file 34 are formed. The data storage part 24, the data analysis part 26, the data processing part 28, the data transmission part 32, and the file receive section 22 are the same as that of what is provided in the Web server of the general former here, In order that the data processing part 30 and the httpd configuration file 34 may realize the authentication system concerning this embodiment, it is the newly added composition. The file about the authentication failure page for reporting that user authentication besides a service content slack Web page went wrong is stored in the file storing part 22. Especially the data processing part 28 is an execution module started by setting out by the httpd configuration file 34, While realizing the access propriety check of the general former in the

analysis of a http header as the 1st-step security check function, the access propriety check based on the contents of the Cookie received from the client 12 as the 2nd-step security check function is performed.

[0023]Next, drawing 3 is a figure showing the composition of the Web authentication server 16. In the figure, the composition of most Web authentication servers 16 is the same as that of Web service server 10, and gives correspondence numerals to corresponding composition. The database 18 for attestation is connected especially to the Web authentication server 16, and the data processing part 30a can perform user authentication by asking this database 18 for attestation, when URL which received is what requires attestation.

[0024]In Web service server 10 first shown in drawing 2 by this authentication system, URL transmitted from the client is received by the data receiving section 24, and the data analysis part 26 of Web service server 10 acquires a name, various variables, etc. of a file which are demanded from URL which received. Then, if it usually becomes, a service content slack predetermined file will be read from the file storing part 22 by the data processing part 28, The place which it is processed if needed and sent out to the Internet by the data transmission part 32 in this Web service server 10. Starting specification of the data processing part 30 is carried out by the httpd configuration file 34, and two steps of access propriety checks are given by this data processing part 30.

[0025]That is, in the data processing part 30, analysis of a http header is first conducted as the 1st-step access propriety check, and whether it being the demand from the client which has [whether URL is transmitted from the IP address of a fixed range and] jp domain, for example, and a matter are checked. And when it does not suit a check here, the Web page showing the purport of an authentication failure is replied to the client 12.

[0026]or [that Cookie is contained in the data which the 2nd more-step access propriety check is performed, and is received from the client 12 on the other hand when it suits this check] -- as for the contents, it is checked what kind of thing it is noting that it is contained. Namely, Cookie which expresses a purport [finishing / user authentication] with this authentication system to the client 12 to which user authentication is normally performed by the Web authentication server 16 is published. On the occasion of access from the client [finishing / user authentication] 12, the Cookie is transmitted to Web service server 10.

[0027]And in Web service server 10, when there is access from the client 12, the contents of the Cookie transmitted from there as the 2nd-step access propriety check are checked. If this check shows that it is access accompanied by the Cookie of a purport [finishing / user authentication], the Web page required of the client 12 will be replied normally. On the other hand, if it turns out that it is access without Cookie of a purport [finishing / user authentication], the redirect request of transmitting a Web page with a META tag to the client 12 will be performed. This META tag is one of the redirect request information over the client 12, For example, "<META HTTP-EQUIV="Refresh" CONTENT="3; It has form like authentication demand .html"> in the URL=Web authentication server 16." In this example, 3 seconds after this demand reaches the client 12, "authentication demand .html" stored in the Web authentication server 16 is accessed.

[0028]Next, in the Web authentication server 16 shown in drawing 3, URL redirected and transmitted from the client 12 is received by the data receiving section 24a, and a name, various variables, etc. of a file which are demanded from URL which the data analysis part 26a received are acquired. And to authentication demand .html, if, access from the client 12 like Web service server 10 the data processing part 30a, As opposed to access which analyzes a http header as the 1st-step access propriety check first, and does not suit this check, The Web page which attached

the META tag required as acquiring the Web page showing the purport of an authentication failure from Web service server 10 is transmitted to the client 12. This META tag is "<META HTTP-EQUIV="Refresh" CONTENT="3, for example.; It has form like "authentication failure .html"> in URL= Web service server 10." In this example, 3 seconds after this demand reaches the client 12, "authentication failure .html" stored in Web service server 10 is accessed.

[0029]On the other hand, when the 1st-step access propriety check is cleared, the data processing part 30a performs user authentication of the client 12 further. May require the method of user authentication as the Web authentication server 16 transmitting the certification information of user ID, a password, etc. from the client 12, and, Predetermined certification information is beforehand received from the client 12 by the Web service server 10 side, It may be made to transmit it to the Web authentication server 16 via the client 12 the redirect request from Web service server 10 to the Web authentication server 16 by the method of setting it as a Cookie header. In the data processing part 30 of the Web authentication server 16, user authentication is performed by asking suitably the database 18 for attestation based on the certification information acquired in this way.

[0030]And if user authentication goes wrong, the data processing part 30a, Predetermined URL is read from a file storing part, and the Web page which performs the redirect request to the URL to the client 12 is transmitted so that the Web page showing the purport of the authentication failure stored in Web service server 10 may be accessed. On the other hand, if it succeeds in user authentication, the data processing part 30 will read predetermined URL from a file storing part, and will transmit the Web page which performs the redirect request to the URL to the client 12 so that the predetermined Web page stored in Web service server 10 may be accessed. Under the present circumstances, the Cookie which expresses a purport [finishing / user authentication] in the header of this Web page that transmits is set up.

[0031]If it carries out like this, when the client 12 will access Web service server 10 after this, The user of the client 12 can receive a desired Web page from Web service server 10 normally, without being collectively transmitted by the Cookie showing a purport [finishing / user authentication], and performing user authentication anew.

[0032]Here, based on the communication sequence diagram shown in drawing 4, an authentication procedure is explained about the case which the inquiry to the Web authentication server 16 from Web service server 10 generates.

[0033]First, if the user of the client 12 inputs URL which requires the service to Web service server 10 (S101), the URL is sent out to the Internet by the client 12 (S102). Then, the check of access propriety is performed by Web service server 10 (S103). And when the access request from the client 10 is judged to be what is not provided with required Cookie in the 2nd-step access propriety check mentioned above, especially, The Web page which includes a redirect request in the client 12 from Web service server 10 is transmitted (S104).

[0034]In response, the client 12 sends out URL to the Internet according to the redirect request, and accesses the Web authentication server 16 (S105). In the Web authentication server 16, while performing the 1st-step access propriety check mentioned above, user authentication is performed (S106).

[0035]And if it succeeds in user authentication, the information on the purport that it has attested will be set as Cookie, and the Web page which includes a redirect request so that Web service server 10 may be accessed again will be transmitted to the client 12 (S107). Under the present circumstances, when user authentication goes wrong, the information showing user authentication having gone wrong is set as Cookie, and it may be made to reply a predetermined

Web page to the client 12. If it carries out like this, access from the client 12 which failed in user authentication, for example with Web service server 10 can be distinguished promptly.
[0036]Then, in the client 12, Web service server 10 is again accessed according to the redirect request included in the Web page which received from the Web authentication server 16 (S108). The Cookie of the purport that it has attested is contained in URL transmitted from a client in this access, It judges that Web service server 10 is access from the client which finished user authentication regularly (S109), and the Web page of a user desire is replied to the client 12 (S110). And in the client 12, the Web page which received is interpreted and a display display is performed.
[0037]When the Cookie of the purport that user authentication went wrong is set up by the Web authentication server 16 as mentioned above, it may be made for Web service server 10 to reply the Web page of the purport of a rejecting access, etc. to access accompanied by this Cookie in S110.
[0038]From the client 12 on which the regular information that it attests is recorded as Cookie as mentioned above, when Web service server 10 has access after that, as for Web service server 10, the inquiry to the Web authentication server 16 is not performed. Drawing 5 is a communication sequence diagram explaining communication between the client 12 in this case, and Web service server 10.
[0039]If the user of the client 12 inputs URL which requires the service to Web service server 10 as shown in the figure (S201), the URL is sent out to the Internet by the client 12 (S202). Under the present circumstances, the Cookie of the purport [finishing / user authentication / already] is recorded on the client 12, and the contents of that recorded Cookie are included in URL transmitted to Web service server 10. Then, the check of access propriety is performed by Web service server 10 (S203).
[0040]And in access of this case, since it is judged that it is access provided with required Cookie in the 2nd-step access propriety check mentioned above, the data about the Web page of a user desire is normally transmitted to the client 12 (S204). And in the client 12, the Web page which received is interpreted and a display display is performed.
[0041]Various modification implementation is possible for the authentication system explained above.
[0042]For example, it may be made to set the information showing the term of validity of the user authentication to the Cookie showing a purport [finishing / user authentication]. If it carries out like this, even if Web service server 10 receives the Cookie showing a purport [finishing / user authentication] from the client 12, If it passes over the term of validity, the client 12 can be required to access the Web authentication server 16 again and to perform user authentication if needed.
[0043]Although the client 12, the service server, and the authentication server were made into the Internet and they were premised on being a thing according to an HTTP protocol in the above-mentioned explanation, This invention cannot be based on the gestalt of a protocol or a network, but can be applied to all the network configurations provided with required composition.
[0044]
[Effect of the Invention]As explained above, since the direct access between a service server and an authentication server is abandoned and it was made to make user authentication perform directly between a client and an authentication server according to this invention, the relations of interdependence of a service server and an authentication server can be lessened. For this reason,

it becomes possible to improve the flexibility of an authentication server and to share this authentication server with two or more service servers.

[0045]According to this invention, since redirect request information was collectively transmitted to the client when an authentication server transmitted the information that it attests to a client, the timing at the time of accessing from a client again to a service server can be provided from an authentication server. As a result, the client 12 becomes possible [accessing to a service server again by making reception of this redirect request information into a trigger], for example.

[0046]According to this invention, since it was made for a client to access an authentication server automatically when a client received redirect request information from a service server, user authentication can be advanced, without the user of a client operating special.

[0047]Since it was made for a client to access a service server automatically according to this invention when a client received redirect request information from an authentication server, A service server can be accessed again, without the user of a client who finished user authentication safely operating special.

[0048]Since according to this invention the information that it attested was transmitted to this service server on the occasion of access to a service server when the client had already received the information that it attests, It can know that the client will succeed in user authentication by the service server side.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the entire configuration of the communications system concerning an embodiment of the invention.

[Drawing 2]It is a figure showing the Web service server concerning an embodiment of the invention with the entire configuration of a communications system.

[Drawing 3]It is a figure showing the composition of the Web authentication server concerning an embodiment of the invention.

[Drawing 4]It is a communication sequence diagram explaining the situation of the inquiry to a Web authentication server from a Web service server.

[Drawing 5]It is a communication sequence diagram explaining communication with the client and Web service server which finished user authentication normally.

[Drawing 6]It is a figure explaining the structure of the user authentication concerning conventional technology.

[Description of Notations]

10 A Web service server and 12 A client, 16 Web authentication server, and 18 Database for attestation.